IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

City of Chicago, Plaintiff, v. Marriott International, Inc. and Starwood Hotels & Resorts Worldwide, LLC, Defendants.	)	Case No. _____

COMPLAINT

Plaintiff City of Chicago files this Complaint to seek relief for the City and its residents because Defendants Marriott International, Inc. ("Marriott") and Starwood Hotels & Resorts Worldwide, LLC ("Starwood") violated the Municipal Code of Chicago ("MCC") by failing to protect Chicago residents' personal information. In support, Chicago alleges as follows:

INTRODUCTION

1. On November 30, 2018, the hotel conglomerate Marriott announced a data breach (the "Data Breach") affecting some 500 million people—the second-largest data breach ever.[1] Marriott admitted that *since 2014*, criminal hackers have had unfettered access to a database that stores personal information about guests

[1] *Marriott Announces Starwood Guest Reservation Database Security Incident*, available at http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/.

who reserved rooms at hotels operated by Starwood, a Marriott subsidiary. During this four-year period, criminals copied and encrypted guests' personal information such as names, mailing addresses, email addresses, phone numbers, passport numbers, birthdates, and credit- and debit-card numbers.

2. Defendants have long been aware of the risk of a data breach. The hotel industry has been a favorite target of criminal hackers due to the industry's massive collection of personal information and reputation for lax security. Indeed, Defendants themselves have been the target of multiple computer-security incidents.

3. Defendants nevertheless failed to implement reasonable safeguards that, on information and belief, could have prevented the Data Breach or at least detected it sooner. As one cybersecurity expert observed: "It's astonishing how long it took [Defendants] to discover they were breached. … For four years, data was being pilfered out of the company, and they didn't notice. They can say all they want that they take security seriously, but they don't if you can be hacked over a four-year period without noticing."[2]

4. Defendants' failures have subjected Chicago residents whose personal information is in Starwood's guest-reservation database ("Chicago Victims") to potential identity theft, financial fraud, and other injuries. At the very least, Chicago Victims will be forced to spend time and money in an attempt to protect themselves against the increased risk of injury caused by Defendants' conduct.

[2] *Breach Puts Hotel Guests' Data at Risk*, available at https://www.arkansasonline.com/news/2018/dec/01/breach-puts-hotel-guests-data-at-risk-2/.

5. To make matters worse, Defendants botched their response to the Data Breach. Marriott waited 83 days after discovering the Data Breach to disclose it to the public and, when Marriott finally did so, used an email address that cybersecurity experts have said exposes victims to an even greater risk of identity theft and financial fraud.

6. In announcing the Data Breach, Marriott's Chief Executive Officer acknowledged that Defendants "fell short of what our guests deserve."[3] Yet as a leading cybersecurity expert observed in discussing the Data Breach, "it sure seems like there aren't a lot of consequences when huge companies that ought to know better screw up massively on security, leaving consumers … to clean up the mess."[4] Chicago therefore brings this action to hold Defendants accountable for their failure to protect Chicagoans' personal information and to ensure that Defendants adopt reasonable security measures that reduce the likelihood and extent of any future data breach.

PARTIES

7. Plaintiff Chicago is a municipal corporation and a home-rule unit organized and existing under the laws of the State of Illinois.

8. Defendant Marriott is a Maryland corporation with its principal place of business in Bethesda, Maryland.

9. Defendant Starwood is a Maryland company with its principal place of business in Bethesda, Maryland.

---

[3] *Marriott Announces Starwood Guest Reservation Database Security Incident*, *supra*.
[4] Krebs on Security, *What the Marriott Breach Says About Security*, available at https://krebsonsecurity.com/2018/12/what-the-marriott-breach-says-about-security/.

JURISDICTION AND VENUE

10. The Court has subject-matter jurisdiction under 28 U.S.C. § 1332 because the matter in controversy exceeds $75,000 and Chicago is a citizen of a different State than Defendants.

11. The Court has personal jurisdiction over Defendants because Defendants have conducted and continue to conduct business in Illinois.

12. Venue is proper under 28 U.S.C. § 1391 because Defendants are subject to personal jurisdiction in this District and thus reside in this District.

GENERAL ALLEGATIONS

I. Defendants Collect Massive Amounts of Personal Information.

13. Marriott is the largest hotel chain in the world, operating more than 6500 properties worldwide.[5]

14. Marriott entered into a merger agreement with Starwood in 2015, completing the acquisition the following year.[6]

15. Starwood operates hotels under brand names such as Sheraton Hotels & Resorts, Westin Hotels and Resorts, W Hotels, St. Regis, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Meridien Hotels & Resorts, Four Points by Sheraton, and Design Hotels. Starwood also operates timeshare properties under the brands Sheraton Vacation Club, Westin Vacation Club, The Luxury

[5] Marriott International, Inc., *2017 Annual Report* at 3, available at http://media.corporate-ir.net/media_files/IROL/10/108017/marriottAR17/pdfs/Marriott_2017_Annual_Report.pdf.
[6] *Id.* at 3, 88.

Collection Residence Club, St. Regis Residence Club, and Vistana.[7] These hotels and properties are referred to collectively as "Starwood Properties."

16. Starwood requires guests who reserve rooms at Starwood Properties to provide personal information about themselves. This information includes guests' names, mailing addresses, phone numbers, email addresses, passport numbers, birthdates, gender, arrival and departure information, reservation dates, communication preferences, account data related to a customer-loyalty program called "Starwood Preferred Guest," and credit- and debit-card numbers.[8] Starwood inputs this personal information into its guest-reservation database.

17. Marriott's privacy policy—which governs Starwood Properties—indicates that Starwood may collect additional information about guests, including data about employers, family members, and social-media activity.[9]

18. Marriott represented to its guests: "We use reasonable physical, electronic, and administrative safeguards to protect your Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the nature of the Personal Data and the risks involved in processing that information."[10]

---

[7] *Marriott Announces Starwood Guest Reservation Database Security Incident*, *supra*.
[8] *Id.*
[9] *Marriott Group Global Privacy Statement*, available at https://www.marriott.com/about/privacy.mi.
[10] *Marriott U.S. Privacy Shield Guest Privacy Policy*, available at https://www.marriott.com/about/global-privacy.mi.

II. Defendants Were on Notice to Protect Against Data Breaches.

19. Criminal hackers have repeatedly exploited vulnerabilities in corporate security to obtain personal information about consumers.

20. Over the last decade, the press has catalogued massive data breaches at companies like Equifax, Uber, and Yahoo.[11] These data breaches have also been the subject of well-publicized governmental investigations.[12]

21. "Long before" the Data Breach, "the hotel industry had earned the dubious reputation as a hospitable place for hackers."[13] Recent data breaches in the industry have included breaches against Hilton, Holiday Inn, and Hyatt.[14]

22. A cybersecurity expert explained that "hotels are an attractive target for hackers because they hold a lot of sensitive information, including credit card and passport details, but often don't have security standards as tough as those of more regulated industries."[15]

23. Experts have criticized the hotel industry for continuing to use "antiquated systems" to store "treasure troves of customer data" due to the "cost" of

---

[11] Taylor Armerding, *The 17 Biggest Data Breaches of the 21st Century*, available at https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

[12] *E.g.*, U.S. House of Representatives Committee on Oversight and Government Reform, *The Equifax Data Breach*, available at https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf.

[13] Patrick Clark, *Marriott Breach Exposes Weakness in Cyber Defenses for Hotels*, available at https://www.bloomberg.com/news/articles/2018-12-14/marriott-cyber-breach-shows-industry-s-hospitality-to-hackers.

[14] Krebs on Security, *Marriott: Data on 500 Million Guests Stolen in 4-Year Breach*, available at https://krebsonsecurity.com/2018/11/marriott-data-on-500-million-guests-stolen-in-4-year-breach/.

[15] *Breach Puts Hotel Guests' Data at Risk*, *supra*.

implementing additional safeguards.[16] In discussing the Data Breach specifically, the U.S. Commerce Secretary similarly observed that "[m]any companies have been scrimping on the cyber-security budget."[17]

24. Defendants themselves were subject to computer-security incidents before and/or during the Data Breach.

25. In 2017, cybersecurity experts uncovered a breach that used malicious software to access Marriott's computer-security team's internal email accounts.[18]

26. Starwood has been a repeat target of hackers:

a. In 2014, cybersecurity experts found on Starwood's computer network an "SQL injection bug"—a serious vulnerability that allows hackers to access the network. Around the same time, hackers on the so-called "dark web" were offering to exploit this vulnerability to Starwood's network.[19]

b. In late 2015, Starwood reported that it had suffered a massive credit-card hack the year before.[20]

c. More recently, a cybersecurity researcher found that Russian cybercriminals stole information from Starwood computer servers. The researcher found that Starwood used easily guessable passwords that could allow hackers to access information on Starwood's servers.[21]

---

[16] *Marriott Breach Exposes Weakness in Cyber Defenses for Hotels*
[17] *Id.*
[18] Thomas Brewster, *Revealed: Marriott's 500 Million Hack Came After a String of Security Breaches*, available at https://www.forbes.com/sites/thomasbrewster/2018/12/03/revealed-marriotts-500-million-hack-came-after-a-string-of-security-breaches/#274977f9546f.
[19] *Id.*
[20] *Id.*
[21] *Id.*

27. Defendants were therefore on notice of the need to adopt reasonable safeguards to protect against, detect, and mitigate the effects of data breaches.

III. Defendants Failed to Protect Chicagoans' Personal Information.

28. On November 30, 2018, Marriott publicly announced the Data Breach. The announcement claimed that on September 8, 2018, Marriott "received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database."[22]

29. After allegedly investigating the alert, Marriott discovered that "there had been unauthorized access to the Starwood network since 2014." Marriott also discovered that criminals "had copied and encrypted information" from Starwood's guest-reservation database "and took steps towards removing it."[23]

30. Marriott initially stated that criminals copied information about "up to approximately 500 million guests who made a reservation at a Starwood property."[24] Marriott later reduced this estimate to "approximately 383 million records as the upper limit for the total number of guest records that were involved."[25]

31. Marriott stated that for approximately 327 million guests, the stolen information included "some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest … account information, date of birth, gender, arrival and departure information, reservation date, and

---

[22] *Marriott Announces Starwood Guest Reservation Database Security Incident*, *supra*.
[23] *Id.*
[24] *Id.*
[25] *Marriott Provides Update on Starwood Database Security Incident*, available at http://news.marriott.com/2019/01/marriott-provides-update-on-starwood-database-security-incident/.

communication preferences."[26] Defendants could have attempted to protect this information by encrypting it but, on information and belief, largely failed to do so. Indeed, Marriott admitted that "approximately 5.25 million unencrypted passport numbers were included in the information accessed by an unauthorized third party."[27]

32. Marriott acknowledged that the stolen information also included about 8.6 million payment-card numbers and expiration dates.[28] Although the payment-card numbers were purportedly encrypted, Marriott admitted that it "has not been able to rule out the possibility" that criminals stole the information needed to decrypt the numbers.[29]

33. On information and belief, Defendants failed to adopt reasonable safeguards that would have prevented the Data Breach and detected it sooner. As one cybersecurity expert put it: "With all the resources" that Defendants have, they "should have been able to isolate hackers" long ago.[30] Indeed, some cybersecurity experts have said that Defendants should have discovered the Data Breach as part of their investigation into the credit-card hack that Starwood announced in 2015.[31]

---

[26] *Marriott Announces Starwood Guest Reservation Database Security Incident*, *supra*.
[27] *Marriott Provides Update on Starwood Database Security Incident*, *supra*.
[28] *Id.*
[29] *Marriott Announces Starwood Guest Reservation Database Security Incident*, *supra*.
[30] David Volodzko, *Marriott Breach Exposes Far More Than Just Data*, available at https://www.forbes.com/sites/davidvolodzko/2018/12/04/marriott-breach-exposes-far-more-than-just-data/.
[31] Robert McMillan, *Marriott's Starwood Missed Chance to Detect Huge Data Breach Years Earlier, Cybersecurity Specialists Say*, available at https://www.wsj.com/articles/marriotts-starwood-missed-chance-to-detect-huge-data-breach-years-earlier-1543788659.

IV. Marriott Botched Its Response to the Data Breach.

34. After allegedly discovering the Data Breach on September 8, 2018, Marriott waited 83 days until publicly disclosing the Data Breach on November 30, 2018. That delay was unreasonable and prevented Chicago Victims from taking steps to protect their personal information in the meantime.

35. To make matters worse, Marriott made two critical mistakes when it finally notified Chicago Victims. First, Marriott emailed Chicago Victims from the address "email-marriott.com." That address is registered to a third party, and cybersecurity experts noted that "there was little else to suggest the email was at all legitimate."

36. Second, as one cybersecurity expert observed, the email address "email-marriott.com" is "easily spoofable."[32] The Federal Trade Commission warned consumers victimized by the Data Breach that "scammers try to take advantage of situations like this" by "send[ing] emails with links to fake websites to try to trick people into sharing their personal information."[33] A press report noted that Marriott's use of the address "email-marriott.com" is so "problematic" that "security experts are filling in the gaps—at their own expense"—by registering similar addresses such as "email-marriot.com" and "email-mariott.com" to educate victims and "make sure that scammers didn't register the domains themselves."[34]

---

[32] Zack Whittaker, *Marriott's breach response is so bad, security experts are filling in the gaps — at their own expense*, available at https://techcrunch.com/2018/12/03/marriott-data-breach-response-risk-phishing/.

[33] Federal Trade Commission, *The Marriott data breach*, available at https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach.

[34] Whittaker, *supra*.

37. Beyond its flawed efforts to notify Chicago Victims, Marriott established a website to address questions about the Data Breach. Marriott failed in this task too: the website had "problems staying online."[35]

V. Defendants' Conduct Has Injured and Will Injure Chicago Residents.

38. Chicago "need not allege injury or causation to state a claim" for violations of the MCC. *City of Chi. v. Purdue Pharma L.P.*, 211 F. Supp. 3d 1058, 1071 (N.D. Ill. 2016). Defendants' conduct has, however, injured Chicago residents.

39. Armed with someone's personal information, criminals can commit identity theft and financial fraud.

40. More than 17 million Americans have their identities stolen each year.[36]

41. Data breaches are a main source of identity theft. About one-third of people who are notified about a data breach discover that criminals used their identities for fraudulent means. And nearly one-half of people whose credit-card information is accessed through a data breach become victims of fraud that same year.[37]

42. The Federal Trade Commission described the financial fraud that identity thieves can commit:

> Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some

[35] *Marriott Hacking Exposes Data of Up to 500 Million Guests*, *supra*.
[36] *E.g.*, U.S. Department of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2014* at 1, available at http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408.
[37] *Id.*

> extreme cases, a thief might even give your name to the police during an arrest.[38]

43. Hackers also sell credit- and debit-card information to criminals who use it to clone credit and debit cards.[39]

44. The United States Department of Justice found that 65% of the 17.6 million identity-theft victims in 2014 suffered a financial loss. Nearly 14% of victims never recouped their losses, with the average out-of-pocket loss totaling $2,895.[40]

45. The Department of Justice observed that identity-theft victims also "paid higher interest rates on credit cards, they were turned down for loans or other credit, their utilities were turned off, or they were the subject of criminal proceedings."[41]

46. Of data-breach victims who fall victim to identity theft, many spend additional time and money trying to mitigate the damage. The Department of Justice concluded that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems"; "resolving the problems caused by identity theft [could] take more than a year for some victims."[42]

---

[38] Federal Trade Commission, *Warning Signs of Identity Theft*, available at https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft.
[39] Krebs on Security, *All About Fraud: How Crooks Get the CVV*, available at https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/.
[40] *Victims of Identity Theft*, *supra.*
[41] *Id.*
[42] *Id.*

47. Beyond the financial cost, the Department of Justice reported that more than one-third of identity-theft victims suffered moderate or severe emotional distress due to the crime and invasion of privacy.[43]

48. Defendants' conduct has substantially increased the risk that Chicago Victims will suffer the foregoing injuries.

49. Chicago Victims are also subject to a substantially increased risk of injuries unique to this Data Breach:

a. "[M]any experts and government officials have expressed concern that the passport numbers" taken in the Data Breach, "in concert with the other personal data compromised by the hack, could pose serious risks of identity theft—and be a threat to national security."[44]

b. Criminals can steal "reward points" that guests accumulated under Starwood's customer-loyalty program. Experts have called it "easy" for hackers to redeem points for gift cards, making loyalty-account information more valuable than social-security numbers on the black market.[45]

50. At the very least, Defendants' conduct requires Chicago Victims to spend time and money in an attempt to prevent identity theft and financial fraud. The Federal Trade Commission suggested that victims of the Data Breach obtain and

---

[43] *Id.*

[44] Taylor Telford, *Marriott will pay for new passports after data breach 'if fraud has taken place'*, available at https://www.washingtonpost.com/business/2018/12/04/marriott-will-pay-new-passports-after-data-breach-if-fraud-has-taken-place/?utm_term=.b6aa4acaedf4.

[45] Jennifer Surane & Katherine Chiglinsky, *All Those Starwood Points You Racked Up at Risk in Marriott Hack*, available at https://www.bloomberg.com/news/articles/2018-11-30/all-those-starwood-points-you-racked-up-at-risk-in-marriott-hack.

review their credit reports for signs of identity theft, carefully review their payment-card account statements, place fraud alerts on credit files, and consider placing credit freezes on credit reports.[46] Defendants' conduct therefore will impose burdens on Chicago Victims for years to come.

VI. The Relief Offered by Marriott Is Inadequate.

51. Marriott's proposed remedies for victims of the Data Breach fall short.

52. Marriott initially offered only the opportunity to enroll in a one-year free subscription to a service called WebWatcher, which monitors internet sites where personal information is shared and alerts consumers if their personal information is found. That offer suffers from several problems.

53. For example, WebWatcher does not alert consumers when new accounts have been opened in their names. Plus, as one cybersecurity expert stated, products that (like WebWatcher) monitor the dark-web "aren't particularly effective at protecting your data."[47]

54. In addition, identity thieves may simply wait until Marriott's one-year offer expires. Cybersecurity experts say that "identity thieves often wait to use the stolen data."[48] "Waiting gives thieves time to collect additional information and build out more robust identity profiles in order to open up credit cards in individuals'

[46] Federal Trade Commission, *The Marriott data breach*, available at https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach.
[47] Octavia Blanco, *Why Marriott's ID Theft Protection May Not Be Enough*, available at https://www.consumerreports.org/identity-theft/why-marriotts-id-theft-protection-may-not-be-enough/.
[48] *Id.*

names, file fraudulent tax returns, or get access to current bank accounts."[49] The U.S. Government Accountability Office similarly explained:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[50]

55. After public officials criticized Marriott's initial response, Marriott suggested that it may reimburse victims for the cost of obtaining new passports if Marriott "determines that fraud has taken place."[51] This suggestion is also inadequate. Some identity-theft experts recommend that victims of the Data Breach "consider renewing their passports" now, without waiting for identity thieves to act.[52] Victims who follow this advice will be unable to show that "fraud has taken place" and thus will be on the hook for the full $110 cost to renew a passport.

COUNT 1
Unfair Practice—Failure to Safeguard Personal Information in Violation of MCC § 2-25-090(a)

56. Chicago incorporates all preceding allegations as if they were set forth herein.

---

[49] Matt Tatham, *A Year After the Equifax Breach: Are You Protecting Your Data?*, available at https://www.experian.com/blogs/ask-experian/a-year-after-the-equifax-breach-are-you-protecting-your-data/.
[50] United States Government Accountability Office, *Personal Information* at 33, available at http://www.gao.gov/new.items/d07737.pdf.
[51] Robert Hackett, *Marriott Says It Will Pay for Replacement Passports After Data Breach. Here's Why That's Likely Baloney*, available at http://fortune.com/2018/12/08/marriott-breach-hack-starwood-passport-pay/.
[52] *Why Marriott's ID Theft Protection May Not Be Enough*, *supra*.

57. The MCC provides: "No person shall engage in any act of consumer fraud, unfair method of competition, or deceptive practice while conducting any trade or business in the city. Any conduct constituting an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act … shall be a violation of this section." MCC § 2-25-090(a).

58. The Illinois Consumer Fraud and Deceptive Business Practices Act declares "unfair or deceptive acts or practices … in the conduct of any trade or commerce" to be "unlawful," regardless of "whether any person has in fact been … damaged thereby." 815 ILCS 505/2.

59. While conducting trade or commerce, Defendants engaged in unfair acts or practices by failing to protect Chicago residents' personal information.

60. While conducting trade or commerce, Defendants engaged in unfair acts or practices by failing to detect the Data Breach promptly.

61. While conducting trade or commerce, Marriott engaged in unfair acts by inadequately responding to the Data Breach.

62. Defendants were aware of the risk of a data breach but, on information and belief, failed to implement reasonable safeguards that would have prevented the Data Breach, detected it sooner, and mitigated its effects.

63. Defendants' conduct offends public policy; is immoral, unethical, oppressive, and unscrupulous; and causes substantial injury to consumers.

64. Defendants' violations of the Illinois Consumer Fraud and Deceptive Business Practices Act constitute violations of MCC § 2-25-090(a).

COUNT 2
Unlawful Practice—Failure to Implement and Maintain Reasonable Security Measures in Violation of MCC § 2-25-090(a)

65. Chicago incorporates all preceding allegations as if they were set forth herein.

66. The MCC provides that an "unlawful practice" under the Illinois Consumer Fraud and Deceptive Business Practices Act "shall be a violation of this section." MCC § 2-25-090(a).

67. The Illinois Consumer Fraud and Deceptive Business Practices Act provides: "Any person who knowingly violates … the Personal Information Protection Act … commits an unlawful practice within the meaning of this Act." 815 ILCS 505/2Z; *accord* 815 ILCS 530/20.

68. Accordingly, a knowing violation of the Illinois Personal Information Protection Act is also a violation of MCC § 2-25-090(a).

69. Section 45 of the Illinois Personal Information Protection Act states: "A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure." 815 ILCS 530/45(a).

70. Defendants are "data collectors" under the Illinois Personal Information Protection Act because Defendants are "corporations" that "handle[], collect[], disseminate[], or otherwise deal[] with nonpublic personal information." *Id.* § 5.

71. Defendants violated Section 45 of the Illinois Personal Information Protection Act by failing to implement and maintain reasonable security measures to protect records that contain personal information concerning Chicago residents from unauthorized access, acquisition, destruction, use, modification, or disclosure.

72. Defendants' violations of Section 45 of the Illinois Personal Information Protection Act constitute violations of MCC § 2-25-090(a).

COUNT 3
Deceptive Practice—Misrepresentations and Material Omissions in Violation of MCC § 2-25-090(a)

73. Chicago incorporates all preceding allegations as if they were set forth herein.

74. The MCC prohibits any "deceptive practice while conducting any trade or business in the city. Any conduct constituting an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act … shall be a violation of this section." MCC § 2-25-090(a).

75. The Illinois Consumer Fraud and Deceptive Business Practices Act provides: "deceptive acts or practices, including but not limited to the use or employment of any deception[,] fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice described in Section 2 of the 'Uniform Deceptive Trade Practices Act' … in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby." 815 ILCS 505/2.

76. While engaged in trade or commerce, Marriott engaged in deceptive acts and practices by representing that Marriott used "reasonable" safeguards to protect Chicago residents' personal information.

77. While engaged in trade or commerce, Defendants engaged in deceptive acts and practices by failing to disclose that Defendants lacked reasonable safeguards to protect Chicago residents' personal information.

78. Defendants intended that the public, including Chicago residents, rely on Defendants' deceptive representations and material omissions regarding the security of the personal information stored in Starwood's guest-reservation database.

79. Defendants' representations and omissions were deceptive because, on information and belief, Defendants did not maintain reasonable safeguards to protect Chicago residents' personal information.

COUNT 4
Unlawful Practice—Failure to Give Prompt Notice of Data Breach in Violation of MCC § 2-25-090(a)

80. Chicago incorporates all preceding allegations as if they were set forth herein.

81. Section 10 of the Illinois Personal Information Protection Act provides: "Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope

of the breach and restore the reasonable integrity, security, and confidentiality of the data system." 815 ILCS 530/10(a).

82. Defendants violated Section 10 of the Illinois Personal Information Protection Act by failing to notify Chicago Victims about the Data Breach in the most expedient time possible and without unreasonable delay.

83. Defendants' violations of Section 10 of the Illinois Personal Information Protection Act constitute violations of MCC § 2-25-090(a).

REQUEST FOR RELIEF

Chicago respectfully requests that the Court enter an order granting the following relief:

A. A declaration that Defendants violated MCC § 2-25-090(a). *See* MCC § 2-25-090(e)(4) (authorizing "an action for injunctive relief");

B. An injunction requiring Defendants to adopt and implement reasonable safeguards to prevent, detect, and mitigate the effects of data breaches. *See id.*;

C. Restitution for Chicago Victims. *See id.* § 2-25-090(e)(4) (authorizing "an action for … equitable relief");

D. A monetary fine awarded to Chicago. *See id.* § 2-25-090(f) ("[A]ny person who violates any of the requirements of this section shall be subject to a fine of not less than $2,000 nor more than $10,000 for each offense. Each day that a violation continues shall constitute a separate and distinct offense to which a separate fine shall apply.");

E. Attorneys' fees and costs awarded to Chicago;

F. Pre- and post-judgment interest awarded to Chicago; and

G. Any other relief that the Court deems reasonable.

JURY DEMAND

Chicago requests a trial by jury of all claims.

Dated: February 14, 2019

Respectfully submitted,

EDWARD N. SISKEL
Corporation Counsel of the City of Chicago

BY: /s/ Jane Elinor Notz

Jane Elinor Notz
Deputy Corporation Counsel
(jane.notz@cityofchicago.org)

Stephen J. Kane
Assistant Corporation Counsel
(stephen.kane@cityofchicago.org)

City of Chicago Department of Law
Affirmative Litigation Division
121 North LaSalle Street, Room 600
Chicago, Illinois 60602
Tel: 312-742-6238/312-744-6934
Fax: 312-742-3832